Správna implementácia bezpečnostných štandardov pre IS VS

Peter Bíro

Ministerstvo financií
Slovenskej republiky

MF SR, BA, júl 2009

Princípy zavádzania bezpečnostných štandardov

- Zdrojové normy – najmä 27001, ale aj ďalšie, ako common criteria a podobne
- Požiadavky sú navrhované rámcovo, aby ich bolo možné aplikovať na ľubovoľnú veľkosť a typ organizácie
- Kvalitatívne naplnenie resp. technické podrobnosti sú v súčasnosti iba v metodikách a odporúčaniach

Princípy zavádzania bezpečnostných štandardov

Krásny, ale ťažko chrániteľný

Princípy zavádzania bezpečnostných štandardov

Funkčný, ale ťažko dosiahnuteľný

Princípy zavádzania bezpečnostných štandardov

Kompromis ?

Princípy zavádzania bezpečnostných štandardov

- Výnos obsahuje už iba povinné požiadavky resp. štandardy
- § 1 - Vzťah k zákonu
- § 2 - Definície
  - Bezpečnostný incident
  - Technické komponenty IS VS, zariadenia IS VS
- § 27 až 41 – Bezpečnostné štandardy (pôvodná piata časť):
  - § 27 až 30 – Štandardy pre architektúru riadenia
  - § 31 až 41 – Štandardy minimálneho technického zabezpečenia

BŠ: Štandardy pre architektúru riadenia

- § 27 – riadenie informačnej bezpečnosti
  - Z pohľadu zabezpečenia kontinuity činnosti organizácie najdôležitejší štandard
  - Organizácia resp. zodpovedné osoby musia:
    - v prvom rade vedieť čo sa chráni (aktíva [majetok, ľudia, nehmotné „vlastníctvo" ako napr. údaje atď.], procesy resp. chod organizácie)
    - prečo to chráni (legislatíva, interné/externé požiadavky atď.)
    - a ako to chráni (organizácia riadenia, politika, opatrenia, skutočnosť)
  - Odporúčaná je kombinácia ostatných požiadaviek ohľadom bezpečnosti (napr. ochrana osobných údajov) v rámci jedného „balíka" bezpečnostných dokumentov
  - Jednotlivé časti bezp. politiky a opatrení je vhodné vecne a logicky rozdeliť – podstatná je prehľadnosť a zrozumiteľnosť

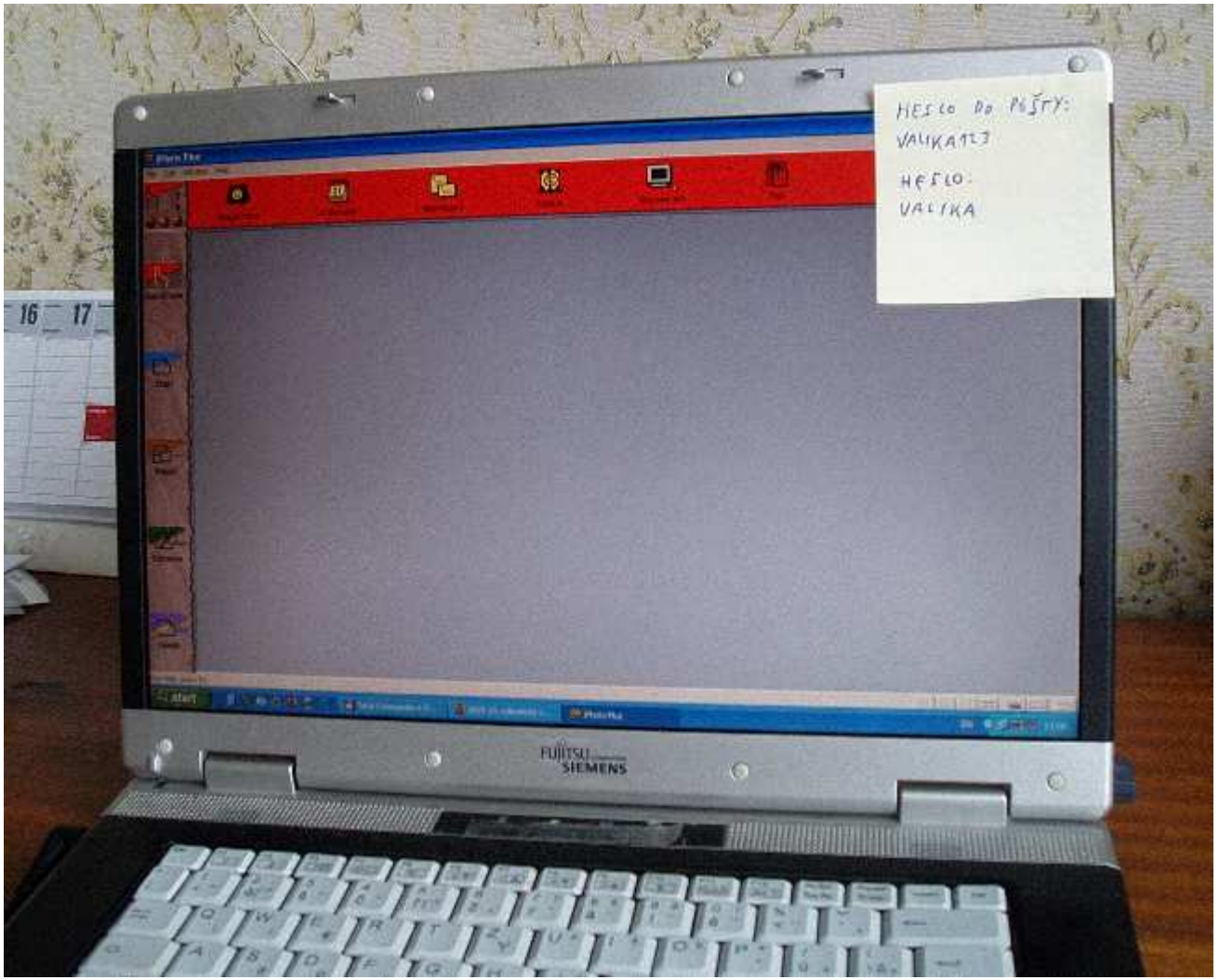
BŠ: Štandardy pre architektúru riadenia

- § 27 – riadenie informačnej bezpečnosti
  - Vyžaduje sa
    - existencia bezpečnostnej politiky s primeraním obsahom, jej vykonateľnosť a dodržiavanie [a) a b)]
    - existencia zodpovednej (riadiacej) osoby s jasne určenými kompetenciami a úlohami, prípadne ďalších osôb s delegovanými (čiastkovými) právomocami [c), d) a e)]
    - Definícia aktív a zodpovednosti za ne [f)]
    - Určenie pozícií (rolí) v IS VS – najmä oddelenie rolí administrátora a „vecného správcu" (správca databázy, gestor, ...) [g)]

BŠ: Štandardy pre architektúru riadenia

- § 27 – riadenie informačnej bezpečnosti
  - Bezpečnostná politika má:
    - Určiť bezpečnostné ciele a spôsoby ich monitorovania a vyhodnocovania [a) 1 a a) 2]
    - Zaistiť podporu vedenia – napr. schválenie v podobe všeobecne záväzného vnútorného predpisu, vyhlásenie o podpore [a) 3]
    - Definícia „bezpečnostných" pozícií v organizácii [a) 4]
    - Zohľadniť a zapracovať všetky právne požiadavky [a) 6 a a) 7]
    - Stanoviť úrovne ochrany IS VS – napr. obyčajné, citlivé (služobné), kľúčové (kritické) (ak je to potrebné) [a) 8]
    - Definovať aktíva a kritické aktíva (ak existujú) [a) 9]
    - Určiť rozsah a periodicitu auditu IB [a) 10]
    - Určiť rozsah a periodicitu zálohovania [a) 11]

Personálna bezpečnosť



BŠ: Štandardy pre architektúru riadenia

- § 28 – personálna bezpečnosť
  - „Amatéri útočia na systémy, profesionáli na ľudí" – sociálne inžinierstvo
  - Poučenie o bezp. politike a povinnostiach (vrátane tretích strán) – pri nástupe, priebežne [a)] – monitorovanie praxe! - www.kry-sa.sk
  - Špecifické školenie alebo poučenie pred vstupom do IS VS (ak je potrebné [b)]
  - Konkrétna zodpovednosť (napr. pracovná zmluva, podpis, špecificky volené funkcie) a vyvoditeľnosť dôsledkov [c) a d)]
  - Ohlasovanie incidentov [e)]
  - Adekvátne ukončovanie pracovného pomeru – odstránenie prístupov, odovzdanie IKT (väčšinou majetková správa), „odovzdanie" el.údajov, vyraďovanie/vymazávanie/likvidácia zariadení [f)]

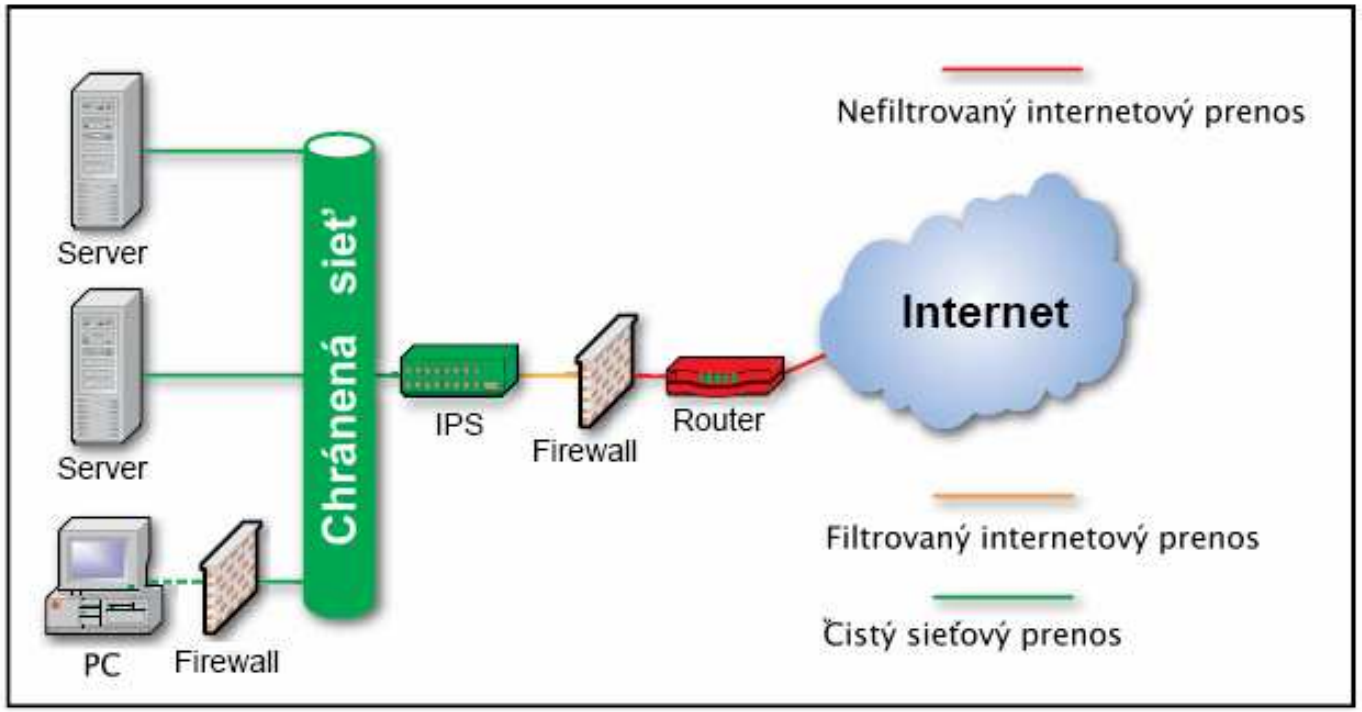
BŠ: Štandardy pre architektúru riadenia

- § 29 – manažment rizík pre oblasť informačnej bezpečnosti
  - Spolu s definíciou aktív základ nastavovania politiky a opatrení
  - Vyžadovaný je systém riadenia rizík a jeho používanie (súčasťou je analýza rizík) a systém monitorovania rizík [a) a b)]
  - Riziká majú zahŕňať aj priestory mimo priestorov organizácie (distribuované pracoviská, infraštruktúra) a riziká v súvislosti s tretími stranami [c) a § 41 a)]
  - Je potrebné mať vypracovanú analýzu závislosti na IS VS (elektronické služby, KRIS) [d)]
  - Definícia kritických procesov a kritických informačných systémov [d) a e)]
  - Havarijné plány, plány na obnovu [f)]
  - Dodržiavanie je v súčasnosti veľmi nedostatočné

BŠ: Štandardy pre architektúru riadenia

- § 30 – kontrolný mechanizmus
  - Všeobecný princíp kontroly – každé „teoretické" opatrenie, cieľ či úloha by mali byť kontrolovateľné, t.j. mať známe ukazovatele kontroly
  - Veľmi častou chybou je najmä nenastavenie merateľnosti dosiahnutia cieľov bezpečnostnej politiky (§ 27, a) 2)
  - Externé audity, ani audity certifikovanou osobou nie sú vyžadované, ale nezávislý audit má väčšiu šancu nájsť chyby [a)]
  - Auditné správy sa majú archivovať a chrániť, ale najmä vyhodnocovať [b)]

Štandardy minimálneho technického zabezpečenia



Je to všetko?

BŠ: Štandardy minim. tech. zabezpečenia

- § 31 + § 34 – Ochrana proti škodlivému kódu + Aktualizácia softvéru
  - Ochrana pred škodlivým kódom (e-maily (vrátane kompresných/šifrovaných súborov), OS, aplikácie, web atď.) [a)]
    - Odhad 20 až 50 mil. zombie PC celosvetovo (rok 2008)
  - Ochrana pred spamom (obojsmerne!) [b)]
    - November 2008 – významný zásah proti spamu – odpojenie serverov spoločnosti McColo – celosvetový dopad bolo zníženie až o 25-50% !!
    - Nechránené PC dostáva priemerne 70 spamových správ denne
    - Spam sa stále vyvíja – v súčasnosti už je možné zaslať spam aj cez kalendáre (Google, Outlook) alebo tlačiareň (dokonca využiť aj fax tlačiarne).
  - Aktualizovaný bezp. softvér [§ 34 a)] v súlade s BP [§ 34 b), § 27 a) 12]

BŠ: Štandardy minim. tech. zabezpečenia

- § 31 + § 34 – Ochrana proti škodlivému kódu + Aktualizácia softvéru
  - Aktualizovaný bezp. softvér [§ 34 a)] v súlade s BP [§ 34 b), § 27 a) 12] – automatizované vs manuálne, záplaty
    - Útočníci sa viac spoliehajú na staré chyby, ako na nové (pri nových je vysoká pravdepodobnosť odstránenia).
  - Iba legálny a povolený softvér – monitorovanie, vrátane mobilných IKT [c)]
  - Pravidlá pre sťahovanie súborov (najmä web) [d)] + monitorovanie
  - Podpora el. podpisu, certifikátov, možnosť kryptovať komunikáciu [e)]
  - Možnosť šifrovania súborov [f)]
    - Šifrovanie na úrovni údajov (skôr doplnkové) alebo diskov (efektívnejšie, výhodné pri ochrane prenosných zariadení)
    - Dôležitá je správa používateľov a kľúčov
    - Problém – spomaľovanie výkonu

BŠ: Štandardy minim. tech. zabezpečenia

- § 32 – sieťová bezpečnosť
  - Firewally – nielen perimeter, ale aj personálne – najmä notebooky
  - 80% bezp. incidentov je zvnútra (chcené/nechcené/umožnené)
  - Evidencia všetkých uzlov [b)] a primeraná ochrana (riadenie prístupu) [c)] – tieto informácie sú citlivé!
  - Vysokým rizikom je internet
    - Nebezpečnosť webov – priemer nebezpečných odkazov celosvetovo je 2%, pri sponzorovaných (sémanticky významnejších) odkazov až viac ako 7%
  - Ochrana po koncový bod, karanténa, rezidentná ochrana

BŠ: Štandardy minim. tech. zabezpečenia

- § 33 – fyzická bezpečnosť a bezpečnosť prostredia
  - Existencia zabezpečeného priestoru – chránený pred vplyvmi, fyzicky oddelený, bez ohrozenia horľavinami, vodou atď. [a), b) a c)]
  - Určenie pravidiel pre prácu v tomto priestore – zákaz vstupu nepovolaným, povolaný iba za určitých podmienok (najmä tretie strany) [d)]
  - Ochrana pre výpadkom elektriny – servery, stanice – UPS, notebooky [e)]
  - Záložné kapacity IS VS + sekundárny priestor (dostatočne vzdialený) – clustre, virtualizácia [f)]
  - Prevádzka IS VS v súlade s predpismi [g)]
  - Pravidlá pre evidenciu tech. komponentov a zariadení IS VS [h) 1]

BŠ: Štandardy minim. tech. zabezpečenia

- § 33 – fyzická bezpečnosť a bezpečnosť prostredia
  - Pravidlá pre používanie zariadení (najmä serverov) na iné účely – zdieľanie aplikácií – napr. virtualizácia [h) 2]
  - Pravidlá pre prenos zariadení v rámci budovy a mimo (notebooky, USB, vrátnica, evidencia) [h) 3 a 5]
  - Vymazávanie a vyraďovanie IKT [h) 4]
    - Prieskum v roku 2007 - 100 HD, z toho 40 nemalo zmazané údaje vôbec alebo boli ľahko obnoviteľné (obsahovali aj citlivé a osobné údaje)
  - Narábanie s el. dokumentmi, USB atď. [h) 6]
    - Podľa jednej medz.štúdie (Ponemon Institute) – 3/5 prepustených zamestnancov v roku 2008 odcudzili dôležité firemné údaje a viac ako 2/3 ich použila pri nástupe
    - Priemerné absolútne straty kvôli strate zákazníkov tvorilo 6,6 mil. dolárov
  - Stanovenie maximálnych dôb výpadku – dostupnosť, robustnosť riešení, kritické IS [i)]

BŠ: Štandardy minim. tech. zabezpečenia

- § 35 – Monitorovanie a manažment bezpečnostných incidentov
  - Bezpečnostný incident – akýkoľvek spôsob narušenia bezpečnosti IS VS, ako aj akékoľvek narušenie BP a pravidiel súvisiacich s bezpečnosťou IS VS
    - V 2008 nastalo napr. vyradenie el. siete niekoľkých miest, havárie električiek kvôli hacknutému diaľkovému ovládaniu, samozrejmosťou je vykrádanie bankových kônt atď.
    - V 2007 prvý masový kybernetický útok na vládne a finančné siete (Estónsko), neskôr ďalšie (Lotyšsko, Gruzínsko)
    - V marci 2006 prvý phishing v Česku (Citibank), neskôr ďalšie dve banky
  - Povinná osoba je zodpovedná za bezpečnosť IS VS (zákon o IS VS)
  - Monitorovanie, evidencia a riešenie bezpečnostných incidentov / výpadkov [a) 1-3, c)] – najviac absentuje práve evidencia

BŠ: Štandardy minim. tech. zabezpečenia

- § 35 – Monitorovanie a manažment bezpečnostných incidentov
  - Vymeniteľnosť evidencie
  - Zavedenie jasného spôsobu ohlasovania a riešenia bezpečnostných incidentov [b), § 28 e)] – slúži aj na zabráneniu využívania sociálneho inžinierstva
  - Kontaktné miesto – aj pre prípadné externé ohlasovanie [e)]
  - Detekcia prienikov – IDS, IPS (povinná pre ministerstvá a ostatné ústredné orgány štátnej správy) [d)]
- § 36 – Periodické hodnotenie zraniteľnosti
  - Hodnotenie slabých miest systému
  - Platforma na pravidelnú výmenu informácií (napr. rada, výbor...)

BŠ: Štandardy minim. tech. zabezpečenia

- § 37 – Zálohovanie
  - Údaje – napr. poštová komunikácia, úradné dokumenty (finálne, rozpracované, typovo od legislatívy cez metodiky až po rozhodnutia), personálne, účtovnícke a majetkové údaje, zmluvy, dokumentácie ku IKT, auditné a bezpečnostné záznamy, atď.
  - Čím viac údajov, tým väčšie problémy s ich rýchlou obnovou
  - Dve strany politiky – ochrana serverov a databáz, ochrana používateľských údajov
  - Archivačná (dlhodobá) záloha (2x, minimálne 1/mesiac, druhá podľa § 38 nie na tom istom mieste), prevádzková (1x, minimálne 1/týždeň) – rozsah daný bezp. politikou [a) a b)]
  - Testy obnovy médií – pri „napaľovaní", automatizované hlásenie, najjednoduchšie testovanie pri HD [c)]
  - Testy obnovy IS VS / 1x rok – živé systémy - čiastočné, praktická pripravenosť [d)]
- § 38 – Fyzické ukladanie záloh
  - Zálohy a licencie - uzamykateľný priestor (napr. „plechová skriňa")

BŠ: Štandardy minim. tech. zabezpečenia

- § 39 – Riadenie prístupu
  - Identifikácia, autentizácia, autorizácia – meno+heslo, ďalšie ochranné prvky (najmä pre mobilné pripojenie – jednorazové SMS heslo, GRID) [a)]
  - Prístup iba tam, kam je to potrebné – vrátane adminov (žiadosť schválená nadriadeným, manažment identít, rozdelenie a nezlučiteľnosť rolí) [b), c), h)]
  - Informovanie o špecifických požiadavkách pre konkrétny IS VS [d)]
  - Logovanie prístupov (odporúča sa aj činnosti), logovanie zmien oprávnení, kontrolovaná zmena logov [d) a i)] – logy neprístupné daným adminom alebo duplikované
  - Pravidlá pre mobilné pripojenie (úplné zakázanie je nevhodné, lepšie je nastavenie pravidiel – trendom vývoja je mobilita [f)]
  - Zabránenie nelegálnemu používaniu – súkromné účely, pornostránky, hackovanie atď. – monitorovanie, upozornenia, „TOP 10“ [g)]

BŠ: Štandardy minim. tech. zabezpečenia

- § 39 – Riadenie prístupu
  - Systémový admin nemá vidieť údaje v databáze (šifrovanie, iná rola typu správca obsahu, databázy t.j. vecný pracovník) [h)]
  - Formalizovaná dokumentácia práv všetkých používateľov (vrátane adminov) – postačuje elektronicky [j)]

BŠ: Štandardy minim. tech. zabezpečenia

- § 40 – Aktualizácia IKT
  - Schvaľovanie zmien a nových systémov (so zahrnutím bezpečnosti) [a)]
  - Jasný zástupca objednávateľa a dodávateľa, žiadna „kolektívna" zodpovednosť – v prípade dodávateľa až na fyzickú úroveň, vrátane dodržiavania BP objednávateľa [b) a c)]
  - Pre malé zmeny stačí jasná politika
  - Dostatočné a zdokumentované testovanie (najmenej 1 týždeň) – pre malé úpravy relevantne [d)]
  - Dokumentácia (používateľská, administrátorská, prevádzková) – dodáva dodávateľ [e] – často krát absentuje najmä prevádzková (konfigurácie, väzby, architektúra)

BŠ: Štandardy minim. tech. zabezpečenia

- § 41 – Účasť tretej strany
  - Najdôležitejšia z pohľadu možnosti úprav IS VS a ochrany financií
  - Analýza rizík zahŕňa aj tretie strany (najmä dodávateľov) [a)]
  - Bezpečnostné požiadavky do zmlúv s dodávateľmi: [b)]
    - dodržanie BP
    - dodržanie platnej legislatívy (je možné explicitne zákona či výnosu)
    - žiadne nevyžiadané funkcie
    - správne nastavené autorské práva a licencie (žiadna neupraviteľná čierna skrinka)
    - vhodná je vzorová zmluva, vždy konzultácia s bezp. manažérom / IT odborom

BŠ: Štandardy minim. tech. zabezpečenia

- § 41 – Účasť tretej strany
  - Kontrola dodržiavania stanovených bezp. požiadaviek – napr. odpočet dodržania bezp. štandardov, nezávislá kontrola [d)]
  - Pri nedodržaní bezpečnostných požiadaviek možnosť neprebrania diela, vypovedania zmluvy, vrátenia zálohy, sankcií [e)]
  - Prístup tretích strán k „živým" údajom podobne ako systémový admin (za konkrétne určených okolností – žiadne svojvoľné aktualizácie či neobmedzený (externý) prístup) [c)]

Kontroly MF SR

- Metodika dostupná na www.informatizacia.sk
  - (menu eGovernment/Štandardy IS VS/Monitorovanie/Bezpečnosť – metodika)
- Hodnotenie štandardov a ich požiadaviek využíva systém váhovania
- MF SR pri kontrole vyžaduje najmä:
  - Dokumentáciu, schopnosť zodpovedať otázky a preukázateľnosť tvrdení
  - Prístup do zabezpečeného priestoru a do IS VS

O B E D